AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 1, line 12 as follows:

In recent years, users ~~are~~ have been able to receive various kinds of services since ~~the~~ network services have come into wide use. Most of those services request that each user ~~inputs~~ input a password. In those services, passwords are used in order to identify if a person trying to receive a particular service is the user himself/herself or not, but users sometimes forget their passwords. In a mail system provided by an administrator on the Internet, when a user has forgotten the password, the user transmits data, besides the password, with which the user can be identified, and when the administrator has authenticated that it is the user himself/herself according to the data, the administrator allows the password to be recovered and presents the password to the user or prompts the user to change the password to a new one.

Please amend the paragraph beginning on page 2, line 18 as follows:

Both of these techniques of the prior art mentioned here have security problems, however, in that a third party who does not know the user's password may be able to obtain the means for recovering the password such as the information to identify the user or the information on key operations, and to recover the password so as to "spoof" as the user or obtain/tamper the data owned by the user using the recovered password.

Please amend the paragraph on page 61, line 12 to page 62, line 3 as follows:

The memory card with CPU 50 performs signature authentication for each transmitted signed document using the signed document and a public key certificate that is stored therein in advance, so as to judge if each document has actually been generated by a guarantor, and if each document is within the expiration period. When it is confirmed that the signed document has been generated by the guarantor and is within the expiration period, the memory card with CPU 50 counts this signed document as one of valid signed documents required for the password recovery. When the count has reached the number of signed documents required for the password recovery, the number being stored in advance, the memory card with CPU 50 reads the encrypted password stored therein in advance, decrypts the read password, and notifies the decrypted password to the mobile phone 60. The signature authentication here is an algorithm that authenticates the signed data generated with a digital signature.

Please amend the paragraph beginning on page 115, line 15 as follows:

In addition, since the master password and the service passwords are encrypted and stored in the memory card with CPU 50 so as to be decrypted when necessary~~; therefore~~, the security level of the memory card with CPU 50 itself is improved.